Datenmanagement lohnt sich – nicht nur für KRITIS Betriebe

IT-Sicherheitsgesetz 2.0 erweitert die Definition für Kritische Infrastrukturen

Georg Seiß M.A.,
Auvesy

Dipl.-Ing. (FH) Nora Crocoll,
Redaktionsbüro Stutensee

Wie lässt sich der Ausfall jener Anlagen und Systeme vermeiden, die zu nachhaltigen Versorgungsengpässen oder sogar zu einer Gefährdung der öffentlichen Sicherheit führen würden? Für diese sogenannten Kritischen Infrastrukturen (KRITIS) machen bspw. das IT-Grundschutzkompendium, die IEC 62443 oder das IT-Sicherheitsgesetz strenge Vorgaben, wie Sicherheitskonzepte systematisch anzuwenden sind. Für die automatisierte Produktion kommt einem durchdachten Daten- und Änderungsmanagement eine immer größere Rolle zu, denn damit lassen sich viele dieser Anforderungen mit einer entsprechenden Lösung verhältnismäßig einfach umsetzen. Zudem kann eine optimierte Datensicherung laufende Kosten drastisch senken.

Momentan umfassen die Kritischen Infrastrukturen (KRITIS) die Bereiche Energie, Gesundheit, Staat und Verwaltung, Ernährung, Transport und Verkehr, Finanz- und Versicherungswesen, Informationstechnik und Telekommunikation, Medien und Kultur sowie die Wasserversorgung. Im Dezember 2020 wurde aber der Entwurf für das neue IT-Sicherheitsgesetz 2.0 vom Kabinett beschlossen und durchläuft nun weitere Gremien. Es ist also absehbar, dass er im Laufe des Jahres 2021 in Kraft treten wird. Dann weitet sich KRITIS wohl aus auf die Abfallwirtschaft und die neu benannten „Infrastrukturen im besonderen öffentlichen Interesse“, also werden vermutlich z.B. auch die DAX-30-Unternehmen auf der Liste der KRITIS-Unternehmen stehen. Betroffene Unternehmen, sollten sich schon jetzt Gedanken darum machen, wie sie dann die notwendigen Vorgaben erfüllen können.

Systematische Sicherheitskonzepte helfen allen

Aber nicht nur Unternehmen, die rechtlich dazu gezwungen sind, für ihre Automatisierungsgeräte und Anlagen entsprechende Anforderungen umzusetzen, sollten sich mit der Frage auseinandersetzen, wie sie sicher produzieren können. Denn die vom BSI gemeinsam mit der Industrie erarbeiteten Sicherheitsmaßnahmen können sich schnell rechnen, bspw. sobald dadurch ein Rückruf oder Anlagenstillstand vermieden wird.

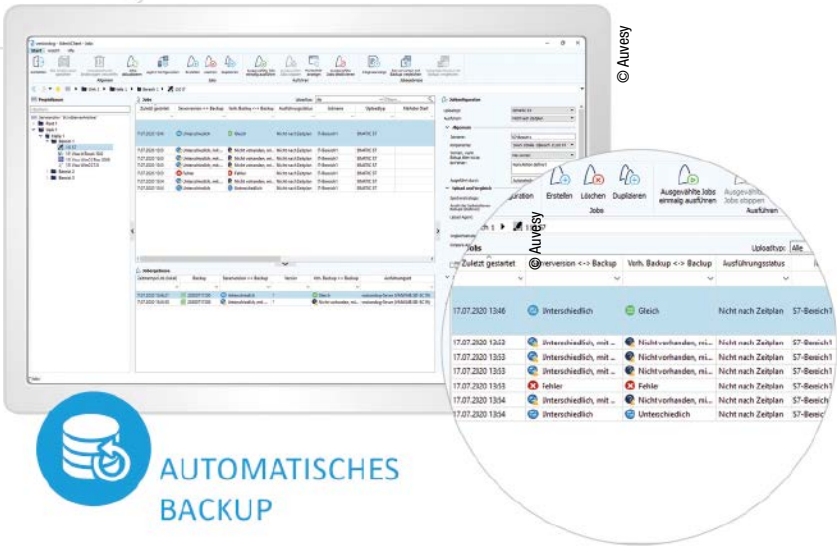
Sicherheit meint in diesem Fall übrigens beides: Die physische Sicherheit (Safety), also der Schutz vor Schäden an Menschen und Dingen und der Schutz vor Datenverlusten oder -manipulation (Security). Oft sind die Grenzen zwischen beiden Bereichen ohnehin fließend – auch bedingt durch die fortschreitende Digitalisierung der Produktion. Mit einer stärkeren Vernetzung zwischen informationstechnischer (IT) und operativer (OT) Ebene gewinnen hohe Sicherheitsstandards an Bedeutung. Der „Defense in the Depth“-Ansatz, der der Normenreihe IEC 62443 zugrunde liegt (siehe Technikkasten), ist hier die oft zitierte Strategie. Für Automatisierungsgeräte und Netzwerkgeräte lassen sich Prävention, Detektion und Reaktion praktisch mit der Software Versiondog des Landauer Softwareherstellers Auvesy umsetzen. Das Datenmanagementsystem stellt für viele Bausteine des IT-Grundschutzes eine Lösung bereit und hilft so, Compliance zum IT-Sicherheitsgesetz herzustellen.

Anforderungen aus IT-Grundschutz-Kompendium zuverlässig erfüllen

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) benennt im IT-Grundschutz-Kompendium verbindliche Maßnahmen für alle KRITIS-Betreiber. Ziel ist es einerseits,

◀ **Abb. 1: Mit einem Datenmanagementsystem wie Versiondog lassen sich in einer heterogenen Automatisierungslandschaft herstellerübergreifend Daten sichern und versionieren.**

Abb. 2: Die Software ermöglicht sowohl die Sicherung, Bereitstellung und Verwaltung von Produktionszahlen durch zyklische Backups als auch Konsistenzprüfung und Alarmfunktion bei Abweichungen. ▼



Defense in Depth – Drei Verteidigungslinien

Beim Defense-in-Depth-Ansatz greifen mehrere Maßnahmen ineinander, um maximale Sicherheit zu erreichen. Den Ansatz kann man sich bildlich wie eine Burg vorstellen: Verschiedene gestaffelte Verteidigungslinien schützen die Burg vor Eindringlingen und anderen Gefahren. Eine erste Verteidigungslinie dient der Anlagensicherheit. Dazu muss der Betreiber organisatorische Maßnahmen treffen, wie physikalische Zutrittsbeschränkungen, Richtlinien und Prozesse zur Nutzung der Anlagen und Kontrollen und sicherstellen, dass diese eingehalten werden. Die zweite Verteidigungslinie betrifft die Netzwerksicherheit. Durch Netzsegmentierung werden Produktionszellen gebildet, die nach außen hin geschützt sind und nur von berechtigten Personen erreicht werden können. Dazu muss der Integrator entsprechende Maßnahmen treffen wie den Einsatz einer Firewall, von Passwörtern oder der Absicherung des externen Zugriffs über VPN. Die innerste Verteidigungslinie wird durch Sicherheitsfunktionen an Geräten bzw. Komponenten der Anlage realisiert. Diese können in sich verschlüsselt oder durch Virenscanner geschützt sein. Dafür zu sorgen ist die Aufgabe des Herstellers.

Anlagenausfälle von vornherein zu vermeiden, egal ob die Ursache auf Problemen mit der Hardware oder Datenmanipulation beruht. Andererseits soll sichergestellt werden, dass bei einem Ausfall ein Neustart der Anlagen schnell und zuverlässig ablaufen kann. Sprich Sicherungen sollen schnell aufzufinden und ebenso einfach einzuspielen sein. Versiondog gewährleistet durch seine Funktionalitäten die Integrität der entsprechenden Daten und Programmierungen. Das Datenmanagementsystem setzt dazu bereits in seiner Grundfunktionalität zahlreiche Anforderungen des Kompendiums um. Dazu einige Beispiele:

Versionierung und Backup

In automatisierten Unternehmen spielen vielfältige Komponenten unterschiedlichster Hersteller zusammen: Klassische PCs, Speicherprogrammierbare Steuerungen (SPS), Industrie-PCs (IPC), Sensoren, Aktoren usw. Diese heterogene Landschaft zu überblicken, ist alles andere als einfach. Mit einem Datenmanagementsystem wie Versiondog wird es jedoch möglich, herstellerübergreifend Daten zu sichern und zu versionieren. Das bedeutet konkret eine standardisierte Verwaltung aller Programmänderungen sowie eine zentrale Ablage aller relevanten Daten als Versionen auf einem Server. Diese Versionen sind dann über einen entsprechenden Client zum Arbeiten zentral verfügbar. Jede abgelegte Version ist für sich konsistent und kann zur Wiederherstellung oder zur Bearbeitung genutzt werden.

Vertraulichkeit, Integrität und Verfügbarkeit von Daten sind nicht nur zur Umsetzung der Industrie 4.0 entscheidend, sondern auch grundlegend für die Qualität von Produkten und der Wettbewerbsfähigkeit eines Unternehmens. Eine Versionierung der Daten ist hierbei ebenso zwingend notwendig wie das regelmäßige Erstellen von (automatisierten) Backups. Die Software ermöglicht sowohl die Sicherung, Bereitstellung und Verwaltung von Produktionszahlen durch zyklische Backups als auch Konsistenzprüfung und Alarmfunktion bei Abweichungen.

Vergleich und Disaster Recovery

Weitere Funktionen wie der Vergleich von Programmständen und die Bereitstellung eines Disaster Recovery sind Strategien, mit welchen die Anforderungen des IT-Grundschutzkompendiums umgesetzt werden können und sich somit Compliance erreichen lässt. Mit verschiedenen Vergleichsszenarien ist es bspw. auch möglich, Datenmanipulation aufzuspüren. Während bei Versionen wissentlich vorgenommen Änderungen miteinander verglichen werden, bilden automatisierte Backups einen

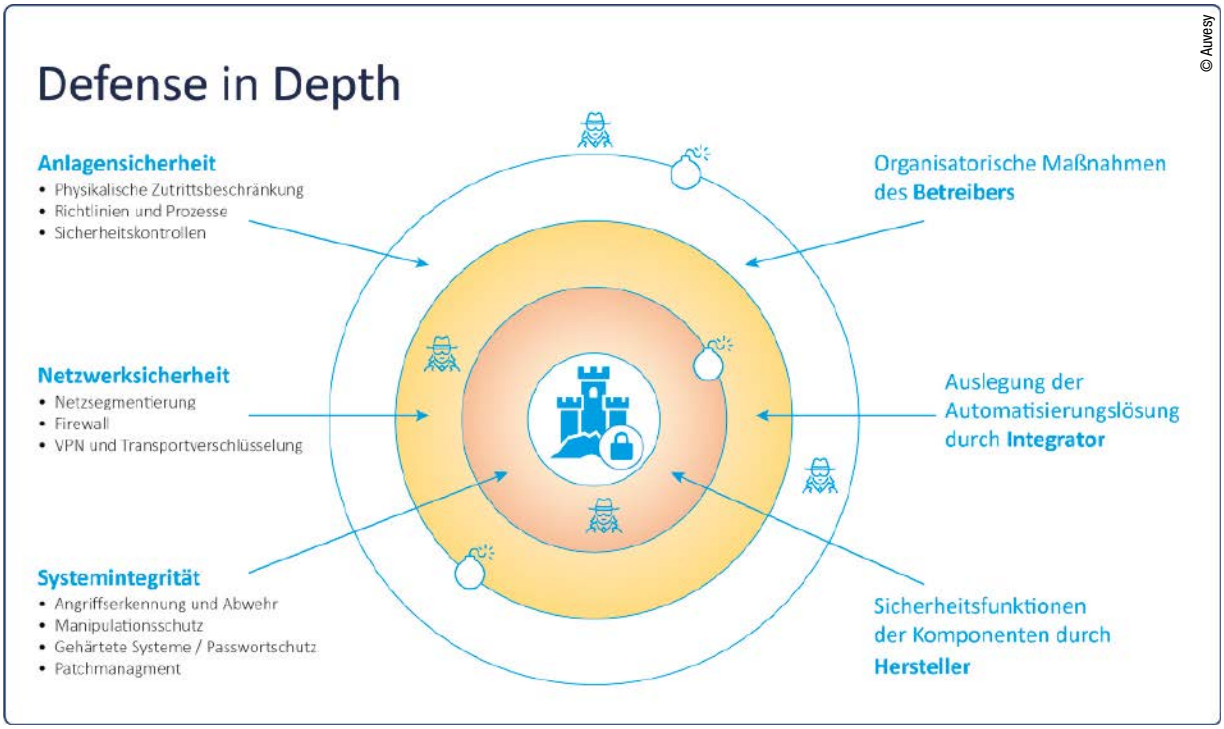


Abb. 3: Beim Defense-in-Depth-Ansatz greifen mehrere Maßnahmen ineinander, um maximale Sicherheit zu erreichen. Der Ansatz kann man sich bildlich wie Schutzwälle einer Burg vorstellen.

Vergleich des Ist- und Soll-Zustandes ab. Diese Szenarien lassen sich übrigens individuell an den Anwendungsfall anpassen.

Ist es aufgrund verschiedener Ereignisse notwendig, den Soll-Zustand bspw. einer Steuerung wiederherzustellen, sollte das schnell gehen. Ein Beispiel: Nach einem Ausfall digital gesteuerter Pumpen in der Abwasserentsorgung müssen Pumpwerksteuerungen so schnell wie möglich wieder in der jeweils aktuellen Version betriebsbereit sein. Denn die weitreichenden Folgen einer längerfristigen Störung im Abwassersystem unter hygienischen bzw. gesundheitlichen Gesichtspunkten liegen auf der Hand. Ein durchdachtes Disaster Recovery ist dann gefragt, um die für ein Unternehmen kritischen Infrastrukturen schnell wieder in Betrieb nehmen zu können. Hier unterstützt das Datenmanagementsystem nicht nur mit einer Strategie zur Reaktion im Fall der Fälle mit einem Backup, sondern hilft über detektive und präventive Maßnahmen bereits im Vorfeld, Ausfälle zu vermeiden.

Notification und Dokumentation

Für den Fall, dass ein Ereignis eingetreten ist, von welchem der Anlagenbetreiber nicht erst bei einer Überprüfung erfahren, sondern proaktiv informiert werden möchte, ermöglicht Versiondog den Versand von Notifications – angepasst an die individuellen Anforderungen. Für eine 100 % Datentransparenz und Nachvollziehbarkeit ist schließlich eine zuverlässige Dokumentation unabdingbar. Zu diesem Zweck ermöglicht das System eine integrierte Dokumentation, eine durchgängige Änderungshistorie und Audit-Trail-Reports auf Knopfdruck.

Einfach installiert

Anwender, die rechtlich nicht gezwungen sind Sicherheitskonzepte umzusetzen, schrecken oftmals vor dem vermeintlichen Aufwand zurück. Dabei ist die eigentliche Installation des Datenmanagementsystems in wenigen Minuten erledigt. Die Integration von Automatisierungsgeräten ist dann nur noch ein wenig Fleißarbeit und abhängig von der Anzahl der Geräte. Aber auch hierfür haben die Landauer Konzepte entwickelt, die eine (teil)automatisierte Integration ähnlicher Geräte möglich machen. Wer den Aufwand gänzlich scheut, kann dies auch einfach als Dienstleistung mitbeauftragen. Verglichen mit dem Aufwand, der durch ein nicht automatisiertes Datenmanagement und die potenziellen Risiken entsteht, rechnet sich der Einsatz eines solchen Systems innerhalb kurzer Zeit. Gleichzeitig steigt nicht zuletzt durch Datentransparenz und konsequente Dokumentation die Produktionsqualität. Auch Unternehmen, die nicht unter das IT-Sicherheitsgesetz 2.0 fallen, sollten daher aus wirtschaftlichen und sicherheitstechnischen Aspekten ihr Datenmanagement mit der Software Versiondog digitalisieren.

Firmeninfo

Der Anbieter von Datenmanagement-Software für automatisierte Produktionsanlagen und Fertigungsprozesse Auvesy wurde im Jahr 2007 gegründet. Mit seinem spezialisierten Softwaresystem „versiondog" bietet das Landauer Unternehmen ein Produkt, das Industrieunternehmen eine einheitliche zentrale Datenablage, vollautomatische Datensicherung, Versionsverwaltung mit detaillierter Änderungserkennung und übersichtlicher Dokumentation bei gleichzeitig hoher Benutzerfreundlichkeit ermöglicht und zugleich auf die Automatisierungssysteme unterschiedlicher Hersteller wie Siemens, ABB, Kuka, Rockwell und Mitsubishi abgestimmt ist.

Die Autoren

Georg Seiß M.A., Business Development Manager, Auvesy
Dipl.-Ing. (FH) Nora Crocoll, Redaktionsbüro Stutensee

Diesen Beitrag können Sie auch in der Wiley Online Library als pdf lesen und abspeichern:
https://dx.doi.org/10.1002/citp.202100529

Kontakt

Auvesy GmbH, Landau
Kristina Gehrlein · Tel.: +49 6341 6810455
Kristina.Gehrlein@auvesy.de · www.auvesy.de
auvesy.com/de/leitfaden-it-grundschutz#c3206